# Interfejsi i protokoli komunikacije u NFC

Tamara Muškatirović-Zekić, Boban Panajotović, Ana Bašić
Služba za tehničke propise, Sektor za regulativu
Republička agencija za elektronske komunikacije
Beograd, Srbija
tamara.muskatirovic@ratel.rs, boban.panajotovic@ratel.rs, ana.basic@ratel.rs

*Sadržaj*—**Novi trend u telekomunikacionoj industriji, NFC koncept je dizajniran tako da združuje više različitih tehnologija, kao što su mobilni telefoni, pametne kartice, čitači kartica, sistemi transakcije i plaćanja,… Na ovaj način omogućava se razmena podataka, samim dodirom sa drugim NFC uređajem istog ili različitog proizvođača. U ovom radu je dat prikaz interfejsa između različitih delova jednog NFC uređaja, kao i protokola komunikacije između dva NFC uređaja sa posebnim osvrtom na bezbednosne protokole. Na početku rada su izložene osnove same tehnologije i dat je kratak opis rada NFC uređaja.**

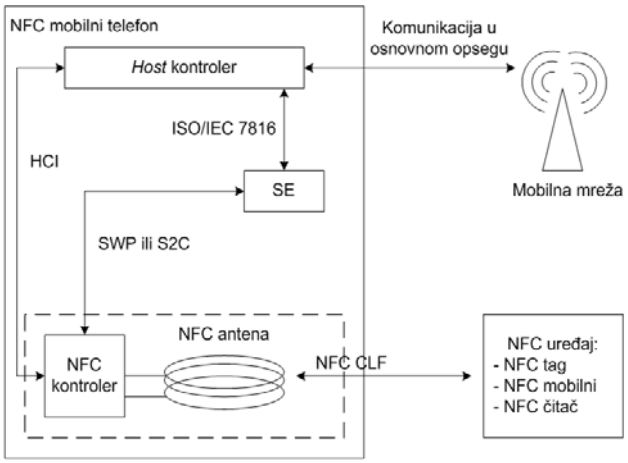
***Ključne reči-NFC; NFCIP; NFC-SEC.***

## I. UVOD

NFC tehnologija je bidirekciona bežična komunikaciona tehnologija kratkog dometa i malog propusnog opsega, između dva NFC uređaja. Komunikacija se vrši na frekvenciji 13.56 MHz, na rastojanju od nekoliko centimetara i pri brzinama prenosa do 424 kbps. Ova frekvencija je prvobitno bila namenjena za RFID (*Radio Frequency Identification*) uređaje koji su sposobni da vrše prenos na udaljenosti od nekoliko metara. Za razliku od RFID tehnologije, NFC komunikacija se odvija samo u neposrednoj blizini.

Glavni motiv za uvođenje NFC tehnologije je integracija ličnih i privatnih informacija, kao što su podaci kreditne ili debitne kartice, u mobilne telefone. Iz tog razloga je bezbednost najvažniji problem, kako bi se sprečilo neovlašćeno prisluškivanje privatnih informacija. Bezbednost je jedna od glavnih karakteristika NFC tehnologije, jer je zbog neposredne blizine dva uređaja verovatnoća presretanja signala mala. Druga važna osobina je sposobnost automatskog uparivanja, što nije bio slučaj sa *bluetooth* tehnologijom. Tako se npr. instalirana aplikacija na mobilnom uređaju automatski startuje kada se pronađe odgovarajući par, tj. aplikacija može biti programirana tako da se startuje automatski čim mobilni uređaj dodirne odgovarajući NFC tag, i može da izvrši sve obrade sve dok nije potrebna intervencija korisnika. Ukoliko nije potrebna intervencija korisnika, u skladu sa ugrađenim algoritmom, aplikacija može da završi svoje procese i da izađe. U tom slučaju, korisnik neće ni primetiti da je aplikacija startovana, procesirana i završena. Ova vrsta obrade nije pogodna za servise sa bezbednosnim zahtevima. Na primer, u slučaju plaćanja je neophodna intervencija korisnika i plaćanje se ne može izvršiti bez saglasnosti korisnika i bez podataka kao što je šifra za plaćanje.

NFC uređaji su: NFC mobilni telefon, NFC čitač i NFC tag [1]. Mobilni uređaj sa integrisanom NFC tehnologijom se obično sastoji od različitih integrisanih kola (ICs – *Integrated Circuits*), sigurnosnih elemenata (SEs – *Secure Elements*) i NFC interfejsa. NFC interfejs se sastoji od beskontaktnog, analogno/digitalnog prednjeg dela koji se zove *NFC Contactless Front-end* (NFC CLF), NFC antene i integrisanog kola koje se zove NFC kontroler. Osim NFC kontrolera, NFC mobilni telefon ima bar jedan SE koji je spojen sa NFC kontrolerom za obavljanje sigurnih transakcija sa spoljnim NFC uređajima. SE pruža dinamično i sigurno okruženje za programe i podatke, i omogućava bezbedno skladištenje vrednih i privatnih podataka, kao što su informacije o kreditnoj kartici korisnika. Takođe, više od jednog SE se može direktno povezati sa NFC kontrolerom. SE-u se može pristupiti i može se kontrolisati interno preko *host* kontrolera, kao i spolja iz RF polja. Na Sl. 1 je prikazana arhitektura NFC mobilnog telefona [2].




Slika 1. Arhitektura NFC mobilnog telefona.

## II. RAD NFC UREĐAJA

Kad se posmatra sama komunikacija, NFC uređaje možemo podeliti na osnovu dva parametra. Prvi parametar je napajanje energijom, i prema njemu uređaje delimo na aktivne i pasivne. Drugi parametar je pokretanje komunikacije i prema njemu uređaje delimo na inicijatore i ciljne uređaje (*target*). Aktivni uređaj je onaj koji je napajan pomoću nekog izvora energije, kao što je baterija, tako da stvara vlastito elektromagnetsko

polje. Sa druge strane, pasivni uređaj je onaj koji nema nikakav integrisan izvor napajanja. Inicijator je onaj uređaj koji inicira komunikaciju, dok ciljni uređaj odgovara na zahtev postavljen od strane inicijatora. Inicijator je uvek aktivan uređaj, jer je neophodan izvor energije za pokretanje komunikacije. Ciljni uređaj, sa druge strane, može biti bilo aktivan ili pasivan. Ako je ciljni uređaj aktivan, onda on koristi vlastiti izvor napajanja kako bi odgovorio, a ako je ciljni uređaj pasivan, on koristi energiju koju stvara elektromagnetsko polje inicijatora koji je aktivan uređaj.

Za ispravnu komunikaciju, NFCIP-1 definiše protokol kojim teče komunikacija između uređaja. Svi uređaji treba da budu u *target* modu i da ne stvaraju RF polje. Uređaj se prebacuje u inicijator mod, samo ako je to potrebno za aplikaciju, i tada aplikacija definiše korišćenje aktivnog ili pasivnog komunikacionog moda. Pre nego što aktivira RF polje inicijator treba da proveri da li postoji drugi aktivni pošiljaoc tako da nijedna druga komunikacija ne bude narušena. Ako se ne detektuje drugo RF polje, inicijator počinje komunikaciju i govori ciljnom uređaju da li da koristi aktivan ili pasivan komunikacioni mod i koju brzinu prenosa da koristi. Nakon komunikacije, oba uređaja se vraćaju u *target* mod i deaktiviraju svoje RF polje.

U NFC tehnologiji, aktivni uređaj stvara RF polje u 13.56 MHz spektru. Kada drugi NFC uređaj priđe dovoljno blizu, posredstvom magnetske induktivne sprege se prenosi energija i podaci sa jednog uređaja na drugi. Induktivna sprega uzrokuje da pasivni uređaj apsorbuje energiju aktivnog uređaja kada priđe dovoljno blizu. Kada se pasivni uređaj pobudi, on može komunicirati i razmenjivati podatke sa drugim uređajem.

Postoje tri osnovna moda rada:

- *Reader/writer* – omogućava da NFC mobilni uređaj razmenjuje podatke sa NFC tagom. Ovaj mod se može podeliti na dva režima rada: režim čitanja i režim pisanja. U režimu čitanja, mobilni uređaj čita podatke sa NFC taga, dok u režimu pisanja, NFC mobilni uređaj upisuje podatke u NFC tag.
- *Peer-to-peer* – omogućava da dva NFC mobilna uređaja razmenjuju podatke međusobno.
- *Card emulation* – omogućava da se NFC mobilni uređaj koristi kao beskontaktna pametna kartica (komunikacija se odvija između NFC mobilnog telefona na jednoj strani i NFC čitača na drugoj strani). Ovaj mod je značajan jer omogućava plaćanje i *ticketing*, i zato što je kompatibilan sa postojećom infrastrukturom pametnih kartica.

## III. INTERFEJSI

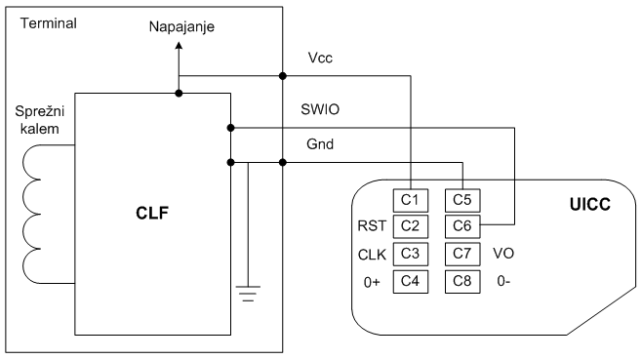
### A. Interfejs između NFC kontrolera i SE

Razvijeni su različiti standardi za NFC komunikaciju, a najperspektivnije opcije za interfejs između SE i NFC kontrolera su SWP (*Single Wire Protocol*) i NFC-WI (*NFC Wired Interface*). Najvažnija razlika između ova dva interfejsa je da SWP koristi jednu fizičku liniju, dok NFC-WI koristi dve linije. Ovde je važno napomenuti da ove dve opcije nisu alternativa jedna drugoj, već su to opcije koje se koriste na određenim mestima.

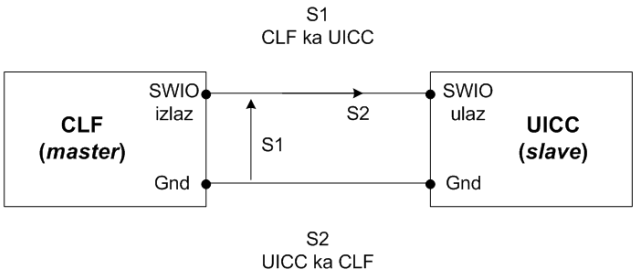
SWP je digitalni *full duplex* protokol, standardizovan u ETSI TS 102 613 [3]. Brzina prenosa podataka je skalabilna od 212 kbps do 1.6 Mbps za razdaljine ispod 10 cm. SWP je *point-to-point* komunikacioni protokol između SE i NFC kontrolera, kao što je prikazano na Sl. 2.

Princip rada je sličan principu *master-slave*, pri čemu se NFC kontroler može posmotrati kao *master* uređaj, a SE kao *slave*. Podaci koji se prenose se predstavljaju binarnim stanjima napona $S_1$ i struje $S_2$ u jednoj žici, kao što je prikazano na Sl. 3. Prenos podataka iz NFC kontrolera ka SE se vrši modulacijom signala $S_1$. U obrnutom smeru, podaci se prenose modulacijom signala $S_2$.

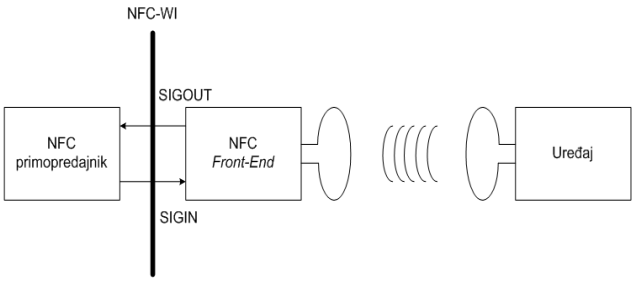
NFC-WI je digitalni žični interfejs, standardizovan u ECMA 373 i ISO/IEC 28361 [4]. NFC-WI definiše SIGIN (Signal-In) i SIGOUT (Signal-Out) žice između primopredajnika, koji je u ovom slučaju SE, i *front-end*-a, koji je u ovom slučaju NFC kontroler, kao što je prikazano na Sl. 4.




Slika 2. CLF-UICC fizički link.




Slika 3. SWP prenos podataka.




Slika 4. NFC-WI arhitektura.

Prema standardu, primopredajnik je entitet koji šalje preko SIGIN žice, a prima preko SIGOUT žice, dok je *front-end* entitet koji šalje preko SIGOUT žice, a prima preko SIGIN žice. NFC-WI interfejs prenosi dva binarna signala koja su definisana kao HIGH i LOW, i podržava tri moguće brzine prenosa podataka 106, 212 i 424 kbps. Pri prenosu brzinom od 106 kbps, niz podataka iz NFC kontrolera ka primopredajniku (SIGIN) nosi logičku I kombinaciju kodiranih podataka sa modifikovanim *Miller* kodom na 13.56 MHz. U suprotnom smeru (SIGIN) niz podataka je kodiran *Manchester* kodom, a zatim obrnut korišćenjem logičke ILI operacije na 848 kHz. Pri prenosu brzinama od 212 i 424 kbps, niz podataka iz NFC kontrolera ka primopredajniku (SIGIN) je kodiran *Manchester* kodom, a zatim obrnut korišćenjem logičke XOR operacije na 13.56 MHz, što odgovara PSK (*Phase Shift Keying*) modulaciji signala takta. U suprotnom smeru (SIGIN), niz podataka je isto kodiran *Manchester* kodom.

Za prenos podataka, NFC koristi tri različite kodne tehnike:

- NRZ-L kodiranje – logička 1 se prikazuje visokim stanjem tokom trajanja jednog bita, dok se logička 0 prikazuje niskim stanjem;
- Manchester kodiranje – pri stanju logičke 1, prva polovina bita je u visokom stanju, a druga polovina bita je u niskom stanju, dok je pri stanju logičke 0 prva polovina bita u niskom stanju a druga polovina u visokom stanju;
- Modifikovano *Miller* kodiranje – pri stanju logičke 1, nizak impuls se dešava nakon polovine trajanja bita, dok se pri stanju logičke 0 nizak impuls dešava na početku bita. Ako logička 0 dolazi nakon logičke 1, ne dolazi do pojave impulsa, pa signal ostaje nepromenjen.

### *B. Interfejs između NFC kontrolera i host kontrolera*

Interfejs između NFC kontrolera i *host* kontrolera je HCI (*Host Controller Interface*), i standardizovan je u ETSI TS 102 622 [5]. HCI ima tri komponente:

- skup *gate*-ova koji razmenjuju komande, odgovore i događaje,
- HCP (*Host Controller Protocol*) mehanizam slanja poruka,
- HCP mehanizam rutiranja koji opciono može da segmentira poruke kada je to neophodno.

*Gate*-ovi predstavljaju ulaznu tačku za servise koji se vrše u *host* kontroleru. Postoje dve vrste *gate*-ova: za upravljanje i generički. Svaki *gate* ima identifikator. *Gate*-ovi komuniciraju jedni sa drugima preko logičkih komunikacionih kanala koji se nazivaju cevi. Postoje dve vrste cevi: statičke cevi i dinamičke cevi. Statičke cevi se ne moraju kreirati i ne mogu se izbrisati. Dok se dinamičke cevi mogu kreirati i brisati. Stanje cevi može biti ili otvoreno ili zatvoreno. Stanje cevi ostaje nepromenjeno čak i ako se napajanje *host*-a ukine i ponovo uspostavi ili ako se *host* ukloni iz mreže. Dužina identifikatora cevi (pID – *pipe identifier*) je 7 bita, i koristi se u zaglavlju HCP paketa za rutiranje informacija. Identifikator cevi kod dinamičke cevi se dinamički definiše od strane *host* kontrolera, dok je identifikator cevi kod statičke cevi unapred definisan. *Host* kontroler koristi vrednost pID kako bi prosledio paket na odredišni *host*. Odredišni *host* prosleđuje paket na odredišni *gate*. Koristeći ovaj mehanizam bilo koja dva *gate*-a koja su spojena preko cevi mogu razmenjivati poruke.

HCP paketi sadrže sledeće segmente:

- CB polje - ima vrednost ″1″ za poslednji paket fragmentirane poruke ili vrednost ″0″ za paket koji pripada fragmentiranoj poruci.
- pID – identifikator cevi.
- poruka – sastoji se iz:
  - zaglavlja poruke koje sadrži instrukciju dužine 6 bita, i polje TIP instrukcije dužine 2 bita. TIP identifikuje vrstu instrukcije. INSTRUKCIJA može biti naredba (type = 0), događaj (type = 1) ili odgovor na komadnu (type = 2).
  - opcionih podataka dužine *n* bita.

Kada je dužina poruke veća od podržane dužine od strane *data link* sloja koristiti se fragmentacija poruke. Poruka će biti podeljena prema sledećim pravilima:

- Svi fragmenti poruka moraju imati zaglavlje paketa.
- Vrednost CB bita u zaglavlju paketa je jednaka 0, osim za paket sa zadnjim delom fragmentirane poruke kada je vrednost 1.
- Samo prvi fragment poruka sadrži zaglavlje poruke.

Izvorni *gate* je odgovoran za fragmentiranje poruke, dok je odredišni *gate* odgovoran za obnovu poruke iz fragmentiranih poruka.

U ETSI TS 102 622 su definisane sledeće procedure:

- Upravljanje cevima – opisuje kako *host* zahteva kreiranje ili brisanje dinamičke cevi između jednog od svojih *gate*-ove i *gate*-a drugog *host*-a.
- Pristup registru – definiše kako *host* može čitati/upisivati parametre u registar drugog *host*-a.
- Pronalaženje *host*-ova i *gate*-ova – definiše kako *host* pronalazi druge *host*-ove i *gate*-ove u mreži.
- Inicijalizacija sesije – definiše kako *host* može otkriti promene u mehanizmima oporavka.

- *Loop back* testiranje – definiše kako *host* može proveriti povezanost sa drugim *host*-om.

### C. *Interfejs između host kontrolera i SE*

Interfejs između *host* kontrolera i SE-a je ISO/IEC 7816. *Host* kontroler postavlja modove rada NFC kontrolera kroz HCI, obrađuje podatke koji su poslati i primljeni, i uspostavlja vezu između NFC kontrolera i SE-a. Osim toga, on održava komunikacioni interfejs, periferne uređaje i korisnički interfejs.

Postoje tri klase rada, u zavisnosti od nominalnog napona napajanja kartice, odnosno SE-a, od strane interfejsnog uređaja, odnosno *host* kontrolera, kroz ulazni napon napajanja VCC. To su:

- klasa A – za VCC=5V,
- klasa B – za VCC=3V,
- klasa C – za VCC=1.8V.

Interakcija između interfejsnog uređaja i kartice se sprovoditi sledećim redosledom operacija: aktivacija, razmena informacija, deaktivacija. Aktivacija se sprovodi tako što interfejsni uređaj primeni klasu radnih uslova na električna kola, tj. podesi odgovarajuće parametre tako da odgovaraju određenoj klasi. Ako kartica podržava klasu, ona će odgovoriti na aktivacione parametre. Za razmenu informacija, kartica i interfejsni uređaj se moraju dogovoriti o transmisionom protokolu i vrednostima transmisionih parametara. Mogući su: *half-duplex* prenos znakova sa interfejsnim uređajem koji je master, *half-duplex* prenos blokova i prenos parova naredba-odgovor. Interfejsni uređaj je zadužen za deaktivaciju.

SE ima sledeće kontakte:

- C1 – ulazni napon napajanja (VCC),
- C2 – ulazni reset signal (RST),
- C3 – ulazni signal takta (CLK),
- C5 – uzemljenje (GND),
- C6 – standardni ulaz (SPU),
- C7 – ulaz/izlaz za serijske podatke (I/O).

Da bi inicirao interakciju sa mehaničkom karticom, interfejsni uređaj treba da aktivira električna kola prema klasi rada, i to sledećim redom: RST treba da postavi u stanje L (*low*), treba da uključi VCC, I/O treba da postavi u prijemni mod, CLK treba da se obezbedi signalom takta. Kada se završi razmena informacija, interfejsni uređaj treba da deaktivira električna kola, i to sledećim redom: RST treba da postavi u stanje L, CLK treba da postavi u stanje L, I/O treba da postavi u stanje L, VCC treba da se deaktiira.

## IV. PROTOKOLI ZA KOMUNIKACIJU IZMEĐU DVA NFC UREĐAJA

Komunikacija između dva NFC uređaja je standardizovana u ISO/IEC 18092 standardu kao NFCIP-1. Ovaj standard definiše samo direktnu komunikaciju uređaj-ka-uređaju, za oba moda rada, pasivan i aktivan. Međutim, RF sloj NFC-a je skup standardnih protokola koji su takođe kompatibilni sa standardom ISO/IEC 14443 (standard za beskontaktne pametne kartice koje rade u neposrednoj blizini) i sa standardom JIS X 6319 kao što je FeliCa (*Sony*-jev standard za beskontaktne pametne kartice koje rade u neposrednoj blizini), kao i sa standardom ISO/IEC 15693 (standard za bliske beskontaktne pametne kartice).

Na fizičkom sloju, NFCIP (*Near Field Communication Interface and Protocol*) je standardizovan u dva oblika:

- NFCIP-1 – koji definiše NFC komunikacione modove na RF sloju i druge tehničke karakteristike RF sloja,
- NFCIP-2 – koji podržava menjanje modova putem detekcije i selektovanja jednog od komuniakcionih modova.

NFCIP-1 je standardizovan u ISO/IEC 18092, ECMA 340 i ETSI TS 102 190 [6]. Ovaj standard definiše dva komunikaciona moda: aktivni i pasivni. Takođe definiše RF polje, interfejs RF komunikacionog signala i opšti tok protokola, početne uslove za podržane brzine prenosa podataka od 106, 212 i 424 kbps.Standard definiše i transportni protokol, uključujući aktivaciju protokola, protokol razmene podataka sa proračunom detkcije greške (CRC za oba komunikaciona moda pri svakoj brzini prenosa podataka) i metode deaktivacije protokola. Noseća frekvencija RF polja je 13.56 MHz. Minimalno nemodulisano RF polje je označeno sa $H_{\min}$ i ima vrednost od 1.5 *A/m* rms. Maksimalno nemodulisano RF polje je označeno $H_{\max}$ i ima vrednost od 7.5 *A/m* rms. Ovo RF polje treba modulisati tokom komunikacije. Komunikaciona šema preko RF interfejsa u aktivnom i pasivnom komunikacionom modu uključuje modulacione šeme, brzine prenosa i kodiranje bita. Pored toga, uključuje i početak komunikacije, kraj komunikacije, prikaz bita i bajta, podelu u frejmove i detekciju greške, detekciju jednog uređaja, izbor protokola i parametara, razmenu podataka i deselekciju NFCIP-1 uređaja. Svi NFCIP-1 uređaji imaju sposobnost komunikacije na 106, 212 ili 424 kbps, i mogu se prebaciti na drugu brzinu prenosa ili ostati na istoj brzini prenosa. Brzina prenosa od inicijatora do cilja i brzina prenosa od cilja do inicijatora ne moraju biti iste za vreme transakcije. Promena brzine prenosa tokom transakcije se može obaviti procedurom promene parametara. Mod (aktivan ili pasivan) se ne može menjati unutar jedne transakcije. Transakcija počinje inicijalizacijom uređaja i prestaje deselekcijom uređaja (ili ekvivalent).

NFCIP-2 je standardizovan u ISO/IEC 21481, ECMA 352 i ETSI TS 102 312 [7]. Standard specificira mehanizam selekcije komunikacionog moda i dizajniran je tako da ne remeti bilo koju komunikaciju koja je u toku na 13.56 MHz za uređaje koji primenjuju ISO/IEC 18092 (tj. NFCIP-1), ISO/IEC 14443 ili ISO/IEC 15693. NFCIP-2 uređaj treba da detektuje spoljašnje RF polje na radnoj frekvenciji, kada je vrednost tog polja iznad praga $H_{threshold} = 0.1875\ A/m$ . NFCIP-2 uređaj ne sme da aktivira svoje RF polje ako otkrije spoljašnji RF signal koji prelazi taj prag. Kada uređaj detektuje spoljašnje RF polje, treba da započne proceduru selekcije moda rada. Ukoliko uređaj ne detektuje spoljašnje RF polje tokom

određenog predefinisanog vremenskog perioda, treba da pokrene sopstveno RF polje i da uđe u odabrani komunikacioni mod.

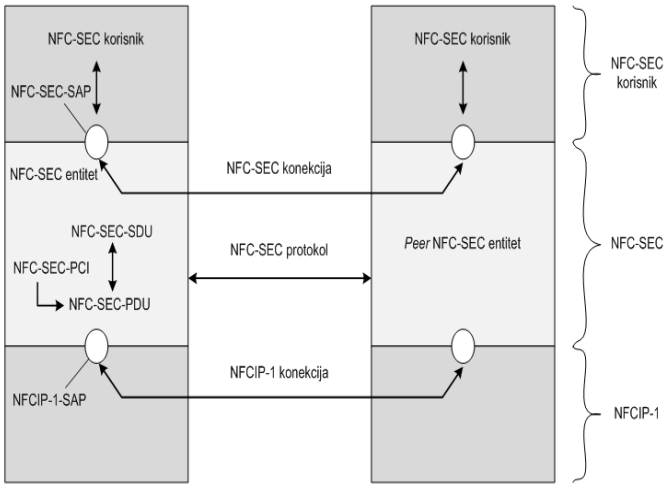
### *A. Bezbednosni protokoli*

Bezbednosni protokoli NFCIP-1 su standardizovani u ECMA 385 kao NFC-SEC [8], i u ECMA 386 kao NFC-SEC-01 [9]. Ovi bezbednosni protokoli se koriste u *peer-to-peer* modu rada.

Protokoli koji su uključeni u NFC-SEC su definisani da se koriste iznad NFCIP-1 protokola. NFC-SEC definiše protokol stack koja omogućava funkcije enkripcije nezavisne od aplikacija na sloju podataka. NFC-SEC je osnovni bezbednosni standard, koji definiše zaštitu od prisluškivanja i modifikacije podataka. Ovaj standard je upotpunjen sa NFC-SEC-01 standardom, koji specificira kriptografske mehanizme koji koriste ECDH (Elliptic Curve Diffie–Hellman) protokol za dogovor oko ključa i AES (Advanced Encryption Standard) algoritam za enkripciju podataka i integritet.

NFC-SEC koristi OSI referentni model specificiran u standardu ISO/IEC 7498-1, kao što je prikazano na Sl. 5.

NFC-SEC korisnici pozivaju i pristupaju NFC-SEC uslugama putem NFC-SAP pristupne tačke (*NFC-SEC-Service Access Point*). NFC-SEC entiteti dobiju NFC-SEC-SDU (*NFC-SEC Service Data Unit*) kao zahtev od NFC-SEC korisnika i vraćaju NFC-SEC-SDU potvrde ka njima. Kako bi obezbedili NFC-SEC usluge, *peer* NFC-SEC entiteti razmenjuju NFC-SEC-PDU (*NFC-SEC Protocol Data Unit*) u skladu sa NFC-SEC protokolom preko NFC-SEC veza. *Peer* NFC-SEC entiteti komuniciraju jedni sa drugima pristupajući NFCIP-1 servisima podataka putem NFCIP-1-SAP pristupnih tačaka (*NFCIP-1 Service Access Point*), i šalju i primaju NFC-SEC-PDU-ove. NFC-SEC-PDU se sastoji od NFC-SEC-PCI (*NFC-SEC-Protocol Control Information*) i jedne NFC-SEC-SDU.




Slika 5. NFC-SEC arhitektura.

Standard ECMA 385 određuje dva tipa usluga koje NFC-SEC obezbeđuje korisnicima. To su: SSE (*Shared Secret Service*) i SCH (*Secure Channel Service*). SSE uspostavlja zajedničku tajnu između dva *peer* NFC-SEC korisnika, koji oni mogu koristiti po vlastitom nahođenju. Pozivanjem SSE se uspostavlja zajednička tajna pomoću sporazuma o ključu i mehanizma potvrde ključa. SCH obezbeđuje siguran kanal. Pozivanjem SCH se uspostavlja ključ veze, izvođenjem iz zajedničke tajne uspostavljene sporazumom o ključu i mehanizmima potvrde ključa, i naknadno se štite sve komunikacije u oba smera preko kanala.

NFC-SEC protokol obuhvata sledeće mehanizme:

- Dogovor o ključu – *peer* NFC-SEC entiteti uspostavljaju zajedničku tajnu koristeći ACT_REQ (zahtev za aktivaciju PDU) i ACT_RES (odgovor na aktivaciju PDU) nakon toga.
- Potvrda ključa – NFC-SEC entiteti potvrđuju svoju dogovorenu zajedničku tajnu koristeći VFY_REQ (zahtev za proveru PDU) i VFY_RES (odgovor na proveru PDU).
- Bezbednost PDU – *peer* NFC-SEC entiteti štite svoje mehanizme razmene podataka koristeći ENC (kodiran paket PDU). Ovaj mehanizam obuhvata integritet sekvence na osnovu zaštićenih brojeva sekvenci, poverljivost, integritet podataka i autentifikaciju porekla.
- Kraj – *peer* NFC-SEC entiteti treba da prekinu svoju sesiju koristeći TMN (raskinuti PDU). Sesija se prekida kada je NFCIP-1 pušten ili poništen, ili kada je NFC uređaj isključen.

Standard ECMA 386 specificira mehanizme za SSE i SCH usluge koje su definisane u standardu ECMA 385. NFC-SEC-01 pruža sledeće funkcije:

- sadržaj poruke sa pravilima spajanja ključeva i drugih polja,
- ključne primitive,
- pravila konverzije i transformacije,
- kriptografski algoritmi i metode.

## V. ZAKLJUČAK

Do danas su sprovedena mnoga NFC testiranja u celom svetu, i to posebno u platnom domenu. Zaključak svih testiranja je da će sa razvojem NFC tehnologije, mobilni telefon postati sigurniji, praktičniji, brži i moderniji uređaj. NFC tehnologija omogućava ljudima da integrišu kartice koje koriste svakodnevno, poput kartice lojalnosti i kreditne kartice, u svoj mobilni telefon. Osim integrisanja kartica u mobilnom uređaju, NFC tehnologija donosi inovacije u oblasti mobilne komunikacije. NFC tehnologija omogućava korisnicima da lako komuniciraju i razmenjuju podatke jednostavnim dodirom dva mobilna uređaja.

Da bi ova komunikacija bila što efikasnija, značajna je standardizacija interfejsa i protokola komunikacije između NFC uređaja različitih proizvođača. Kao što je izloženo u ovom radu, NFC forum zadužen za razvoj nove tehnologije, prati globalno prihvaćene ISO, ETSI i ECMA standarde.

Značajno je napomenuti da, iako postoji skup standarda i specifikacija kojima je opisan rad NFC tehnologije, postoji potreba za daljim usavršavanjem i poboljšanjem istih i iz tog razloga neophodna je saradnja vodećih kompanija i učesnika NFC ekosistema.

## LITERATURA


[1] Tamara Muškatirović-Zekić, Ana Bašić i Boban Panajotović, "NFC tehnologija", International Multidisciplinary Scientific Conference EUROBRAND (7; Zrenjanin; 2013), ISBN 978-86-88065-29-0.

[2] Vedat Coskun, Kerem Ok and Busra Ozdenizci, "Near Field Communication From Theory to Practice", John Wiley & Sons Ltd, 2012.

[3] Recommendation ETSI TS 102 613 – Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 11), (12/09).

[4] Standard ECMA-373 – Near Field Communication Wired Interface (NFC-WI), (June 2006).

[5] Recommendation ETSI TS 102 622 – Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) (Release 11), (12/10).

[6] Recommendation ETSI TS 102 190 – Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1), (03/03).

[7] Recommendation ETSI TS 102 312 – Near Field Communication Interface and Protocol-2 (NFCIP-2), (04/02).

[8] Standard ECMA 385 – NFC-SEC: NFCIP-1 Security Services and Protocol, (10/06).

[9] Standard ECMA 386 – NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES, (10/06).


## ABSTRACT


New trend in telecommunication industry, NFC concept is designed to combine several different technologies, such as mobile phones, smart cards, card readers, transaction and payment systems, ... In this way, you can exchange data just by touching other NFC device of the same or a different manufacturer. In this paper, the interface between the different parts of a NFC device and protocols of communication between two NFC devices, with special emphasis on security protocols, is presented. At the beginning, fundamentals of the technology and a brief description of the work of NFC devices, are presented.


## INTERFACES AND COMMUNICATION PROTOCOLS IN NFC


Tamara Muškatirović-Zekić, Boban Panajotović, Ana Bašić